UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/857,218	06/22/2001	Ryuji Ishiguro	209462	6422

22850 7590 06/14/2006

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/857,218	ISHIGURO ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *28 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *11-20,22-29,38-44 and 50-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11-20,22-29,38-44 and 50-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 3/28/2006, applicant amends claims 11 and 50; cancels claims 1-5 and 21; and adds claims 51-52. The following claims 11-20 and 22-29, 38-44 and 50-52 are presented for examination.

1.1 Applicant's arguments, pages 12-21, filed on 3/28/2006, with respect to the rejection of claims 1-50 have been fully considered but they are not persuasive. With respect to claim 11, Applicant argues that the device of Zhang is a cable television receiver and as explained in the last office action, Zhang discloses other features of receiver 20 such as implementation as a PC, etc. (see column 3, lines 1-35) and the POD module may be a smart card among other electronic devices disclosed. In response to applicant's argument that combining Zhang and Sims to use the same key for authentication and obtaining data would necessitate a substantial redesign, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). In response to applicant's request about public-key encryption providing more security than symmetric key encryption and also providing authentication, applicant is provided with prior art that discusses the teaching as mentioned in the last Office action. Applicant has amended claim 11, which new limitations, which are not

supported by the specification as, explained below and the rejection of this claim is further explained below. Applicant also adds claims 51-52, with regard to these claims and the other independent claims not amended, Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Upon further consideration 11-20 and 22-29, 38-44 and 50-52 are still rejected in view of the same references.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 51 and 52 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Examiner is unable to locate where in the specification the claimed limitations of claims 51 and 52 are described as claimed. The specification does not seem to provide support for the apparatus as claimed and the additional features. It is also not clear in light of the specification what element or elements applicant refers to by the first key and the second key.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

3.1 Claims 11, 51 and 52 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3.2 Claim 52 depends upon data processing apparatus of claim 1, which is a cancelled claim.

3.3 Claims 11, 51 and 52 are rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention. Evidence that claims 11, 51 and 52 fail(s) to correspond in scope with that which applicant(s) regard as the invention can be found in the reply filed 3/28/2006. In that paper, applicant has stated the contents data is acquired using second key data and authentication is performed using the same second key, and this statement indicates that the invention is different from what is defined in the claim(s) because applicant's disclosure does not describe the same exact key being used for acquiring data and authentication.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 1-5, 11-22, 25-29, 38-44, and 50** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,550,008 to **Zhang et al** in view of US Patent Publication US 2002/0016919 to **Sims, III**.

4.2 **As per claim 11, Zhang et al** discloses a method for furnishing key data to a data processing apparatus, comprising:

In one embodiment, **Zhang et al** discloses receiving second key data different from said first key data, for example (see column 13, line 55 through column 14, line 8); and wherein said second key data is used for acquiring contents data furnished from said contents server for storage in said data processing apparatus, said second key data also being used for authentication of said data processing apparatus and said portable reproducing apparatus in order to effect transmission/reception of the contents data from said contents server, for example (see column 13, line 55 through column 14, line 50), (see also column 10, line 10-30). As shown above, key data received from the server, allow authentication of both devices to take place and derivation of key for acquiring contents data from the server. **Zhang et al** substantially teaches at least three

devices: a content server, POD module (any device connected to a host or integrated circuit device, a smart card, etc.) that meets the recitation of data processor or portable reproducing apparatus and a host device (any device that has a receiver such as a video cassette recorder, personal computer etc.) that meets the recitation of portable reproducing device or data processing apparatus, for example (see column 3, lines 1-35); it is understood that they could be interchanged, and further discloses that the devices are not limited to the examples and the invention is not limited to television broadcast system but any other system including other audio/video transmission using means such as the Internet etc., for example (see column 2, lines 49-67).

Zhang et al discloses in one embodiment receiving secret keys and random seeds that meets the recitation of first key data, and they are stored in the storage elements of the POD and the host for authentication; (see column 11, lines 28-51). In another embodiment **Zhang et al** discloses receiving (binding information that meets the recitation of first key data (see column 6, lines 25-46) to said data processing apparatus (host), the data processing apparatus is operable to reproduce content; thus, it inherently contains a contents reproducing program is installed, for example (see column 3, lines 9-13); authentication between the data processing apparatus and portable reproducing apparatus (POD) is performed based on the binding data (see column 6, lines 47-50). **Zhang et al** discloses that encrypted information transmitted from the server (head-end system) is stored in storage elements (such as compact disc) (column 7, lines 15-30) sensitive information is protected by the binding information (see column 7, lines 45-63). It is apparent that information in the storage elements can be retrieved from the key data received.

Although the invention discloses key derivation for acquiring the content using a shared key, **Zhang et al** suggests that the invention is not limited to a specific crypto scheme, for example (see column 2, lines 12-48 and column 4, lines 20-36). **Zhang et al** also suggests in another embodiment two different sets of key data furnished by a server one for authentication and another for encryption of content, for example (see column 12, lines 8-22). Therefore it would have been obvious to one skilled in the art at the time the invention was made to modify the invention of **Zhang et al** to use public/private key scheme for encrypting the data instead of generating symmetric key data in the device as public/private key provides more security and at the same time provides authentication between the two entities as known in the art. It is also very well known in the art that the use of key pair including a public key for authentication and a private key for encryption as disclosed for example by Schneier in "Applied Cryptography" . Therefore, for the above reasons, these modifications would have been obvious to one of ordinary skill in the art of cryptography without departing from the spirit and scope of the invention as suggested by **Zhang et al**. **Zhang et al** teaches encrypted contents data received from the head end can be stored in an external recording medium for storage such as a compact disc (see column 7, lines 15-30 and 44-51) also discloses the POD decrypting content data received from a provider according to key access protocol (column 3, lines 25-44), but was silent about the POD retrieving the data from the storage element (CD) because it is obvious that if the data is stored in the CD it must be retrieved using a key. It is apparent to one of ordinary skill in the art at the time the invention was made that a content key may be used to access the data from the storage element. **Sims, III** in an analogous art discloses media content protection wherein a content provider sends content key and authentication keys the content is accessed from a media

device using a disk key or content key (page 8, paragraph 81 and page 9, paragraph 98) and discloses to execute the content a public key (authentication key) and content key are needed (page 6, paragraphs 54-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Zhang et al** to restrict access to the media by using a key to acquire the content from the media, as taught by **Sims, III** (page 9, paragraph 98). One of ordinary skill in the art would have been motivated to do so because it would add security to the content and at the same time ensures that only authorized devices are allowed to use the encrypted content thus the source of the media would have some control of whether the media device is authorized for using the content as suggested by **Sims, III** (page 9, paragraphs 95 and 98).

As per claims 22 and 38, Zhang et al discloses when contents reproducing apparatus (POD) transmits/receives contents data distributed from a content server, second key data different from first key data is furnished over a network and being used for authentication in acquiring contents data furnished from said contents server, for example (see column 13, line 55 through column 14, line 8 and column 14, lines 20-50); (see also column 10, line 10-30). As shown above, key data received from the server, allow authentication of both devices to take place and derivation of key for acquiring contents data from the server.

Zhang et al discloses the host configured to acquire content data from storage elements storage elements (such as compact disc column 7, lines 15-30) and furnishing content data to the portable reproducing apparatus (POD) (see column 11, lines 28-51). **Zhang et al** discloses in one embodiment receiving secret keys and random seeds that meets the recitation of first key

data, and they are stored in the storage elements of the POD and the host for authentication; (see column 11, lines 28-51). In another embodiment **Zhang et al** discloses receiving (binding information that meets the recitation of first key data (see column 6, lines 25-46) to said data processing apparatus (host), the data processing apparatus is operable to reproduce content; thus, it inherently contains a contents reproducing program is installed, for example (see column 3, lines 9-13); authentication between the data processing apparatus and portable reproducing apparatus (POD) is performed based on the binding data (see column 6, lines 47-50). **Zhang et al** discloses that encrypted information transmitted from the server (head-end system) is stored in storage elements (such as compact disc) (column 7, lines 15-30) sensitive information is protected by the binding information (see column 7, lines 45-63). It is apparent that information in the storage elements can be retrieved from the key data received.

Although the invention discloses key derivation for acquiring the content using a shared key, **Zhang et al** suggests that the invention is not limited to a specific crypto scheme, for example (see column 2, lines 12-48 and column 4, lines 20-36). **Zhang et al** also suggests in another embodiment two different sets of key data furnished by a server one for authentication and another for encryption of content, for example (see column 12, lines 8-22). Therefore it would have been obvious to one skilled in the art at the time the invention was made to modify the invention of **Zhang et al** to use public/private key scheme for encrypting the data instead of generating symmetric key data in the device as public/private key provides more security and at the same time provides authentication between the two entities as known in the art. It is also very well known in the art that the use of key pair including a public key for authentication and a private key for encryption as disclosed for example by Schneier in "Applied Cryptography" .

Therefore, for the above reasons, these modifications would have been obvious to one of ordinary skill in the art of cryptography without departing from the spirit and scope of the invention as suggested by **Zhang et al**. **Zhang et al** teaches encrypted contents data received from the head end can be stored in an external recording medium for storage such as a compact disc (see column 7, lines 15-30 and 44-51) also discloses the POD decrypting content data received from a provider according to key access protocol (column 3, lines 25-44), but was silent about the POD retrieving the data from the storage element (CD) because it is obvious that if the data is stored in the CD it must be retrieved using a key. It is apparent to one of ordinary skill in the art at the time the invention was made that a content key may be used to access the data from the storage element. **Sims, III** in an analogous art discloses media content protection wherein a content provider sends content key and authentication keys the content is accessed from a media device using a disk key or content key (page 8, paragraph 81 and page 9, paragraph 98) and discloses to execute the content a public key (authentication key) and content key are needed (page 6, paragraphs 54-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Zhang et al** to restrict access to the media by using a key to acquire the content from the media, as taught by **Sims, III** (page 9, paragraph 98). One of ordinary skill in the art would have been motivated to do so because it would add security to the content and at the same time ensures that only authorized devices are allowed to use the encrypted content thus the source of the media would have some control of whether the media device is authorized for using the content as suggested by **Sims, III** (page 9, paragraphs 95 and 98).

As per claim 17, Zhang et al substantially teaches at least three devices: a content server, POD module (any device connected to a host or integrated circuit device, etc.) that meets the recitation of data processor and a host device (any device that has a receiver such as a video cassette recorder, personal computer etc.) that meets the recitation of portable reproducing device, for example (see column 3, lines 1-35); it is understood that they could be interchanged, and further discloses that the devices are not limited to the examples and the invention is not limited to television broadcast system but any other system including other audio/video transmission using means such as the Internet etc., for example (see column 2, lines 49-67). **Zhang et al** also discloses transmission of keys for authentication and content protection that meets the recitation of first master and authentication key, for example (see column 15, line 30 through column 16, line 12 and column 12, lines 8-22). **Zhang et al** also discloses second set of keys different from the first keys for authentication between the first and the second device. Although the invention discloses key derivation for acquiring the content, the invention is not limited to a specific crypto scheme, for example (see column 2, lines 12-48 and column 4, lines 20-36). In one embodiment **Zhang et al** discloses second key sets with at least two keys for authentication and transmission/reception of the contents data, for example (see column 4, line 20 through column 5, line 30).

As per claims 16 and 42, Zhang et al discloses the limitation of using key data for decrypting the content received from a content server that meets the recitation of wherein said second key is a server connecting key for downloading contents from a contents server, for example (see column 10, lines 10-30).

As per claims 18-20 and 25-27, Zhang et al discloses the limitation of wherein said first key data is furnished from an external storage medium, for example (see column 4, line 37 through column 5, line 19; column 5, line 50 through column 6, line 35).

As per claims 2, 13, 29, 44, Zhang et al substantially teaches updating keys, for example (see column 2, lines 42-48) and substantially teaches the limitation of wherein the portable device holds authentication keys and master keys and keys being furnished to reproducing program over the network and further teaches said portable reproducing device performing reciprocal authentication with said reproduction program using the authentication key of the same generation as discussed above. **Zhang et al** does not explicitly teach the reproducing device holding first to i'th authentication keys updated in generation from the first to the i'th generation, i being an integer equal to 2 or larger. However, **Sims, III** in an analogous art discloses a portable reproducing device holding generations of keys, for example (see page 9, paragraphs 0093-0097; page 10, paragraphs 0107-0108; page 13, claims 22-23). **Sims, III** further discloses that by having a list of authorized keys and updating means this invention not only provides protection, but also provides limited access of content. For instance, list of authorized keys may be updated by communication with an external source to allow a media device to securely provide content key to a decoder not originally included as an authorized decoder, for example (see page 3, paragraph 0022), in addition media devices may be allowed to generate their own protected content. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Zhang et al** to

provide a reproducing device holding generation of keys, as taught by **Sims, III**. The motivation to do so is given by **Sims, III** because by having a list of authorized keys and updating means the invention as combined would not only provide protection, but also provide limited access of content; list of authorized keys may be updated by communication with an external source to allow a media device to securely provide content key to a decoder not originally included as an authorized decoder, for example (see page 3, paragraph 0022), in addition media devices may be allowed to generate their own protected content as suggested by **Sims, III**.

Claims 3-5, and 43, recite the same inventive concept as claim 2 and therefore they are rejected on the same rationale as the rejection of claims 2 7, 13, 44, 49 above.

As per claims 12, 14, 28, 39, 40, and 50, these claims recite similar limitations as found in claims 2 and 11, except for using ID information and key data of plural generations. **Zhang et al** discloses the limitation of using ID to generate and update new key data that meets the recitation of wherein the ID information of said portable reproducing apparatus and key data of an ith generation are transmitted to said data processing apparatus and wherein the generation of key data of said portable reproducing apparatus is updated based on the ID information of said portable reproducing apparatus, for example (see column 9, lines 1-50; and column 8). **Sims, III** further discloses storing key data of plural generations therefore these claims are rejected on the same rationale as the rejection of claims 2 and 11.

As per claims 15 and 41, Zhang et al discloses the limitation of using a compact disk for storage and processor for using key data for accessing the content that meets the recitation of wherein the first key is a ripping key for ripping contents from a compact disc, for example (see column 7, lines 1-30).

5. **Claims 23-24** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,550,008 to **Zhang et al** in view of US Patent Publication US 2002/0016919 to **Sims, III** as applied to claim 22 and further in view of US Patent 6,751,598 to **Yagawa et al**.

5.1 **As per claims 23-24, Zhang et al** discloses installing the application and routines from an external storage to perform the copyright control of the invention that meets the recitation of wherein said contents reproducing program is included in a comprehensive management unit processing the copyright management, said comprehensive management unit being stored by being installed from an external storage medium, for example (see column 10, lines 10-30). **Yagawa et al** in an analogous art discloses wherein said contents reproducing program is included in a comprehensive management unit processing the copyright management, said comprehensive management unit being stored by being installed from an external storage medium and also discloses wherein key data is settled at the same time as said comprehensive management unit is installed in order to prevent an illegal copy from being distributed, which meets the recitation of wherein key data for the 0th generation as said first key data is acquired at the same time as said comprehensive management unit is installed, , for example (see column 6, line 30 through column 7, line 46; column 12, lines 4-18; see also column 11, lines 1-35 for

processing copyright management using user ID and key data). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Zhang et al** to have key data for the 0th generation as said first key data acquired at the same time as said comprehensive management unit is installed, in order to prevent an illegal copy of the digital content from being distributed, as taught by **Yagawa et al**. One skilled in the art would have been motivated to do so as suggested by **Yagawa et al** so as to prevent tampering during installation and to prevent illegal copy of the digital content from being distributed, for example (see column 7, lines 19-46).

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6.1 **Claims 51-52** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Publication US 2002/0016919 to **Sims, III**.

As per claim 51, Sims, III discloses a data processing apparatus connected to a compact disc and a portable reproducing apparatus, comprising: a first unit configured to obtain a first key used for copying first content stored on the compact disc (100) (see page 3, paragraphs 19-22); a second unit configured to read the first content from the compact disc (see page 4, paragraphs 34 and 37); a receiver configured to receive, from a key server, a second key for receiving second content distributed from a content server (see page 3, paragraphs 19-22); **Sims, III** discloses different embodiments may be used such as receiving public key, secret key, or content key from server; control unit configured to copy and store the first content on the compact disc with first key, and copy and store the second content data distributed from the content server with the second key. **Sims, III** discloses content data from the server to be stored may be encrypted with content key that meets the recitation of second key (page 8, paragraph 88); and further discloses media key that also meets the recitation of first key for copy and store content from the compact disc (see page 8, paragraph 81). Figure 1 comprises control program and processor for performing the steps of copying and storing (see page 4, paragraphs 36-37)

As per claim 52, Sims, III discloses a data processing apparatus such as a computer further comprising: a transmitter configured to transmit copied first content data to a portable reproducing apparatus (111) or an external memory as known in the art; **Sims, III** discloses disc authentication between the playback device and the media device using the disk key (see paragraphs 113-114) that meets the recitation of an authentication unit configured to perform authentication by using the first key between the data processing apparatus and the portable reproducing apparatus in case of transmitting the first content data from the compact disc. **Sims,**

III also discloses for pay-per-view content which is content from the content server authentication with public/private key protocol may be used that meets the recitation of using the second key in case of transmitting the second content data from the content server between the data processing apparatus and the portable reproducing apparatus (see page 11, paragraph 123 and claims 14-15).

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
June 11, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100